EXHIBIT 21

X CORP (TWITTER INC.) ASSESSMENT
FOR THE PERIOD OF MAY 26, 2022, THROUGH MAY 25, 2023

FTI Cybersecurity

An Intelligence-Led, Expert-Driven, Strategic Approach to Global Cybersecurity Challenges

Table of Contents

I. Introduction

X Corp. ("Twitter" or "X" or the "Company" or the "Respondent") is subject to a Decision and Order ("Order"), in a matter brought by the United States ("U.S.") Federal Trade Commission ("FTC"), Docket No. C-4316. The Order, effective May 26, 2022, resulted from the FTC's determination that it had reason to believe Respondent had violated the Decision and Order the FTC previously issued in *In re Twitter, Inc.,* C-4316, 151 FTC LEXIS 162 (F.T.C. March 2, 2011) and the FTC Act.

Provision V of the Order requires Twitter to establish and implement, and thereafter maintain for twenty years, a comprehensive information security and privacy program (the "Program") designed to protect the privacy, security, confidentiality, and integrity of Personal Information. Requirements of the Program are outlined in Provision V.A-I.

Provision VI of the Order requires Twitter to obtain initial and biennial assessments ("Assessments") from a qualified, objective, independent third-party professional ("Assessor") who meets the requirements outlined in Provision VI. Each Assessment must be completed within sixty days after the end of the reporting period to which the Assessment applies. Twitter engaged FTI Consulting, Inc. ("FTI" or "we" or "our") as the Assessor to perform this initial Assessment.

Provision VII of the Order requires Twitter to cooperate with the Assessor. The Company shall not withhold any material facts from the Assessor, and must not misrepresent, expressly or by implication, any fact material to the Assessor's: (1) determination of whether Respondent has implemented and maintained the Program required by Provision V of the Order, titled Mandated Privacy and Information Security Program; (2) assessment of the effectiveness of the implementation and maintenance of Provisions V.A-I; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Program.

As of June 2022, Twitter established its Program, made up collectively of the Information Security Program and the Privacy and Data Protection ("PDP") Program, by implementing information security and privacy controls ("Controls") intended to meet or exceed the protections required by Provision V of the Order. Most Controls were considered implemented on or before November 7, 2022, which is in accordance with the requirements of the Order. Details of this Program are outlined in Section V of this report titled Twitter's Information Security and Privacy Program Overview. The content within Section V has been wholly provided by Twitter, and FTI is not responsible for the contents, comments, or conclusions in Section V. FTI has reviewed Section V and does not have any reason to believe that it is inaccurate.

The purpose of this Assessment is to determine whether the Program and its underlying Controls are designed and implemented effectively, operate as intended, and produce outcomes to meet the requirements of the Order. FTI performed inquiry, inspection, examination, and observation of the Controls to assess the effectiveness of the Program and to determine whether the Controls

implemented meet or exceed the protections required by Provision V of the Order. This Assessment applies to the period May 26, 2022, through May 25, 2023 ("reporting period").

On October 27, 2022, Twitter, which at the time was a publicly traded company, was acquired by Elon Musk and became a privately held company (the "October 2022 Acquisition"). Following the October 2022 Acquisition, organizational restructuring occurred at Twitter, primarily throughout November and December 2022. The restructuring and accompanying strategy changes impacted the leadership, organization, and operation of the Program, including multiple departures of individuals that designed and operated Controls within the Program. While the Program operated continuously throughout the reporting period, in our Assessment, we identified multiple gaps and weaknesses in the design and operation of the Program, many of which were caused, at least in part, by the organizational restructuring that occurred, the significant loss in personnel, and the sudden nature in which the restructuring was executed.

II. Report of Independent Assessor

In accordance with Provisions VI and VII of the Order between Twitter and the FTC, FTI has assessed the establishment, implementation, and maintenance of the Program. This Assessment applies to the reporting period of May 26, 2022, through May 25, 2023.

Our Assessment is focused on the overall Program, which includes both the PDP Program and the Information Security Program. The development of the criteria and Controls outlined in the Program are based on domains and functions that make up relevant privacy and information security frameworks. PDP Controls are based on a combination of the following: the International Organization for Standardization ("ISO") 27701, 27002, and 29184 control frameworks; and the Privacy Management Framework ("PMF") based on the Generally Accepted Privacy Principles created by the American Institute of Certified Public Accountants ("AICPA"). Information Security Controls are based on the ISO 27001 and 27002 control frameworks. Twitter has tailored certain Controls to specific business functions, products, and the Twitter operating environment. FTI noted that the totality of the Controls outlined in the Program extend above and beyond the scope of the Order, which demonstrated Twitter's commitment to maintaining industry-standard and comprehensive privacy and information security programs.

As part of this Assessment, the Company is responsible for the content found in the section titled "Twitter's Information Security and Privacy Program Overview." Our responsibility is to express our conclusions with respect to the requirements of the Order.

Our Assessment was conducted in accordance with privacy and information security best practices, relying on published guidance from ISO, AICPA, the Information Systems Audit and Control Association ("ISACA"), and the U.S. National Institute for Standards and Technology ("NIST"), including the NIST Special Publication 800-30 "Guide for Conducting Risk Assessments" Revision 1.

Our Assessment examined evidence supporting the effectiveness of the Program. We believe that our Assessment provides a reasonable basis for our opinion, and we did not rely solely on the assertions or attestations made by Twitter's management. We are not responsible for Twitter's interpretation of, or compliance with, information security or privacy-related laws, statutes, or regulations applicable to Twitter in the jurisdictions within which Twitter operates. We are also not responsible for Twitter's interpretation of, or compliance with, information security or privacy-related self-regulatory frameworks. Therefore, our examination did not extend to the evaluation of Twitter's interpretation of, or compliance with, information security or privacy-related laws, statutes, regulations, and self-regulated frameworks with which Twitter has committed to comply.

Twitter has implemented and maintained the Privacy and Information Security Program required by Provision V of the Order. The Program, as designed, is comprehensive in that it provides sufficient coverage across all relevant privacy and information security domains and is in alignment with the ISO

27701 and ISO 27001/02 frameworks, respectively, upon which the Program is based. As currently designed, the Controls that make up the Program are only partially tailored to the Twitter operating environment, meaning that the scope of certain Controls are not clearly defined as to what activities within Twitter's environment they apply. Additionally, a lack of internal documentation of Control design and operation made evidencing the Controls difficult and, for some Controls, not effective. One root cause of this systemic observation is the organization restructuring and reduction in staff that occurred at Twitter after the October 2022 Acquisition. In addition to publicly reported departures of Program leadership, multiple staff-level departures and terminations required many Controls to be assigned to new Control Owners in a short amount of time. Program staff and Control Owners communicated to FTI throughout the Assessment period that the reduction in staff caused temporary gaps in Control operation and led to a lack in overall visibility within the Program. We also found multiple Controls that were owned and operated by only one or a small number of Twitter employees and that procedural documentation was not adequate in the possible event of additional departures or terminations.

In addition to the Program being based on requirements outlined in the Order and the ISO 27001/02 and ISO 27701/02 frameworks, Twitter has implemented privacy and information security risk management strategies to identify relevant risks to the privacy, security, confidentiality, and integrity of Covered Information and implement Controls intended to sufficiently reduce those risks. We found Twitter's information security risk assessment to be comprehensive. [redacted] Twitter has developed a multi-year information security and privacy strategy with the goal of continuing to mature the Program, both through risk-based short-term solutions and broader enterprise transformation.

Twitter has designed multiple pathways for monitoring and assessing the sufficiency and effectiveness of the Controls within the Program. [redacted], was envisioned as part of the Program. However, primarily due to lack of resources and the disbandment of its internal audit function, Twitter did not complete an assessment of the Program in the 12 months prior to the end of

the reporting period as originally intended. FTI noted that Twitter has reported that it has since completed contracting with a service provider to provide outsourced audit support, which will include these second-line assessment activities. FTI also noted that Twitter completed relevant assessments of impacted Controls in the aftermath of Covered Incidents during the reporting.

Based on FTI's interviews with Company personnel and Assessment of the overall Program, we found that Twitter continues to prioritize privacy and information security as foundational within the organization. FTI interviewed Twitter's new CEO, Linda Yaccarino, who was appointed in June 2023; Twitter Global Data Protection Officer, Renato Monteiro, who transitioned into the role in November 2022; and Twitter's current Security Engineering Lead, Christopher Stanley. FTI also interviewed key Control Owners and strategic stakeholders responsible for designing and implementing Twitter's privacy and information security strategies. A consistent tone was evident throughout these interviews: that privacy and information security are crucial tenets of the company culture in order to achieve long-term success and trust with users. [redacted] FTI found that Twitter's long-term approach and strategy were effective given Twitter's industry, scale, and threat landscape. We noted that Twitter has also implemented multiple pathways by which Twitter reviews changes to regulatory requirements and implements controls as required, which is particularly evidenced by procedures adapted to adhere to the defined requirements by the European Union ("E.U.") General Data Protection Regulation ("GDPR"), a federal data protection regulation.

This report is intended for the information and use of the management of Twitter, the FTC, and other third parties who receive the report from Twitter for an authorized purpose.

Tracy Wilkison
FTI Consulting, Inc.
July 25, 2023
Los Angeles, CA

III. Requirements for Third Party Assessor

Provision VI.D of the Order states that each Assessment must:

1. Determine whether Respondent has implemented and maintained the Program required by Provision V of the Order, titled Mandated Privacy and Information Security Program;
2. Assess the effectiveness of Respondent's implementation and maintenance of Provisions V.A-I;
3. Identify any gaps or weaknesses in, or instances of material noncompliance with, the Program;
4. Address the status of gaps or weaknesses in, or instances of material non-compliance with, the Program that were identified in any prior Assessment required by this Order;[1]
5. Identify specific evidence (including, but not limited to, documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is: (a) appropriate for assessing an enterprise of Respondent's size, complexity, and risk profile; and (b) sufficient to justify the Assessor's findings. No finding of any Assessment shall rely primarily on assertions or attestations by Respondent's management. The Assessment must be signed by the Assessor, state that the Assessor conducted an independent review of the Program and did not rely primarily on assertions or attestations by Respondent's management. To the extent that Respondent revises, updates, or adds one or more safeguards required under Provision V.E of this Order during an Assessment period, the Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard.

A. Summary Findings Related to Provision VI.D.1 of the Order

Per the Order, Twitter established and implemented the Information Security Program and the PDP Program. Collectively, these individual programs make up the Program and are designed to protect the privacy, security, confidentiality, and integrity of Covered Information.

Twitter's PDP Program, published on June 19, 2022, is based on a combination of the ISO 27701 framework and Privacy Management Framework.

Twitter's Information Security Program, published on June 30, 2022, is based on the security principles of confidentiality, integrity, and availability to protect critical data, systems, and other sensitive assets. The Information Security Program is made up of security Controls that are aligned to a combination of industry frameworks, primarily the ISO 27001/02 frameworks.

[1] Note – As this is the first third party assessment under this Order, FTI does not address Provision VI.D.4 in this Report.

Twitter's description of the Program is detailed in Section V of this report.

We found the design of the Program to be comprehensive. Our conclusion is based on the following observations:

- Our review of Twitter's documented PDP Program and Information Security Program did not find gaps in the strategic design of the Program. The Program is based on industry-recognized frameworks. The Program is also communicated and distributed to Twitter leadership as well as Twitter employees.
    - We noted that the PDP Program and Information Security Program documents were approved and signed by designated Program leads who departed the Company around the time of the October 2022 Acquisition and subsequent organizational restructure. Designated Program leads who have managed and been responsible for the Program since then have maintained the PDP Program and Information Security Program documents as initially approved.
- Our review of Twitter's documentation did not find gaps in application and asset scoping. The Program applies to Twitter's production and corporate technology environments as well as to all products, services, features, and experiments. Where applicable, the Program applies to contractors and service providers contracted by Twitter.
- Our review of Twitter's information security risk management strategy and the information security risk assessment (ISRA) completed in June 2022 found alignment with a risk taxonomy derived using the ISO 27002 control set, which includes relevant assignments of inherent risk, Control strength, and residual risk.
- Our review of Twitter's documentation found that Twitter did not complete an enterprise-wide privacy risk assessment in the 12 months prior to the close of the reporting period. [redacted]
- Our review of Twitter's inventory of Controls did not find gaps when mapped against the industry-recognized ISO 27001/02, 27701, and Privacy Management Framework. Our Assessment found gaps and areas of improvement for the Program, including in both the design and operation of certain Controls, which we outline in Sections III.B and III.C of this report.
    - We noted that, throughout the Assessment, Twitter continued to identify necessary modifications to Controls to tailor them to specific Twitter operations or clarify applicability (i.e., Controls scoped to production or corporate assets) and made changes to Control ownership where needed.

To summarize, our Assessment found that Twitter has implemented and maintained a Program required by Provision V of the Order.

We reviewed and assessed 260 Controls across 15 information security control domains:

1. Information Security Policies;
2. Organization of Information Security;
3. Human Resource Security;
4. Asset Management;
5. Access Control;
6. Cryptography;
7. Physical and Environmental Security;
8. Operations Security;
9. Communications Security;
10. System Acquisition, Development and Maintenance;
11. Supplier Relationships;
12. Information Security Incident Management;
13. Information Security Aspects of Business Continuity Management;
14. Compliance; and
15. Acquisition Risk Management.

We reviewed and assessed 69 Controls across nine privacy control domains:

1. Management;
2. Agreement, Notice, and Communication;
3. Collection and Creation;
4. Use, Retention, and Disposal;
5. Access;
6. Disclosure to Third Parties;
7. Security for Privacy;
8. Data Integrity and Quality; and
9. Monitoring and Enforcement.

Collectively, the Program contains 329 Controls that were assessed by FTI. A small number of Controls were deprecated during the reporting period upon Twitter's determination that the Controls did not apply to Twitter's operating environment. FTI reviewed and agreed with the Control deprecation decisions. We found that all assessed Controls were implemented during the reporting period. We found that multiple Controls operated with exception during the reporting period, with notable gaps in Program effectiveness in the months immediately following the October 2022 Acquisition and subsequent organizational restructuring and reduction in force. A detailed assessment of each Control is provided in Section VI of this report.

We found that the Program established and implemented by Twitter is appropriate. Our observation is that Twitter has identified the relevant control frameworks to be leveraged in protecting the privacy, security, confidentiality, and integrity of Covered Information as required by the Order.

B. Summary Findings Related to Provision VI.D.2 of the Order

To determine the effectiveness of Twitter's implementation and maintenance of Provisions V.A-I, we performed tasks designed to:

- Assess the sufficiency and applicability of the Controls to determine whether Twitter's obligations with the Order are met;
- Assess the design effectiveness of the Controls to determine whether the relevant risks are addressed;
- Assess the operating effectiveness of the Controls to identify gaps or weaknesses; and
- Validate that the Controls were in place at the relevant times throughout the reporting period.

Our opinion is that throughout the reporting period of May 26, 2022, through May 25, 2023, Twitter implemented and maintained the safeguards required by Provisions V.A-I of the Order. Throughout the reporting period, there were instances where Controls did not operate effectively. The Controls assessed for each subsection of Provision V of the Order are listed below.

Provision V.A *Document in writing the content, implementation, and maintenance of the Program;*

[redacted]

Provision V.B *Provide the written program, and any evaluations thereof or updates thereto to Respondent's board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of Respondent responsible for the Program at least once every calendar quarter;*

[redacted]

Provision V.C *Designate a qualified employee or employees to coordinate and be responsible for the Program;*

[redacted]

Provision V.D *Assess and document, at least once every twelve (12) months and promptly following the resolution of a Covered Incident (not to exceed ninety 90 days after the discovery of the Covered Incident), internal and external risks to the privacy, security, confidentiality, or integrity of Covered Information that could result in the: (1) unauthorized collection, maintenance, use, disclosure, alteration, destruction of, or provision of access to Covered Information; or the (2) misuse, loss, theft, or other compromise of such information;*

The safeguards for this requirement include those in Controls B.1.3.4, B.1.4.3, B.1.4.5, B.3.4.1, 16.1.1, 16.1.2.a, 16.1.2.b, 16.1.3.a, 16.1.4.a, 16.1.4.b, 16.1.5, 16.1.6.b, 18.2.1, 18.2.2.a, 18.2.2.b, 18.BP.1.a, 18.BP.1.b, and 18.BP.3.

[redacted]

Provision V.E *Design, implement, maintain, and document safeguards that control for the material internal and external risks Respondent identifies to the privacy, security, confidentiality, or integrity of Covered Information identified in response to Provision V.D. Each safeguard must be based on the volume and sensitivity of Covered Information that is at risk, and the likelihood that the risk could be realized and result in the: (1) unauthorized collection, maintenance, use, disclosure, alteration, or destruction of, or provision of access to Covered Information; or the (2) misuse, loss, theft, or other compromise of such information.*

[redacted]

Provision V.E.1 *Prior to implementing any new or modified product, service, or practice that collects, maintains, uses, discloses, or provides access to Covered Information, conducting an assessment of the risks to the privacy, security, confidentiality, or integrity of the Covered Information;*

[redacted]

Provision V.E.2 *For each new or modified product, service, or practice that does not pose a material risk to the privacy, security, confidentiality, or integrity of Covered Information, documenting a description of each reviewed product, service, or practice and why such product, service, or practice does not pose such a material risk;*

T[redacted]

[redacted]

Provision V.E.3 *For each new or modified product, service, or practice that poses a material risk to the privacy, security, confidentiality, or integrity of Covered Information, conducting a privacy review and producing a written report ("Privacy Review") for each such new or modified product, service, or practice. The Privacy Review must:*

[redacted]

In addition, FTI found that Twitter has defined certain safeguards included in privacy and information security Controls that also align with specific requirements contained in Provisions V.E.3(a)-(n):

[redacted]

FTI's summary of findings pertaining to Provisions V.E.3 and subsections(a)-(n) can be found below the following list of the Provisions.

Provision V.E.3(a) *Describe how the product, service, or practice will collect, maintain, use, disclose, or provide access to Covered Information, and for how long;*

Provision V.E.3(b) *Identify and describe the types of Covered Information the product, service, or practice will collect, maintain, use, disclose, or provide access to;*

Provision V.E.3(c) *If the Covered Information will be collected from a User, describe the context of the interaction in which Respondent will collect such Covered Information (e.g., under security settings, in pop-up messages in the timeline, or in response to a prompt reading, "Get Better Ads!");*

Provision V.E.3(d) *Describe any notice that Respondent will provide Users about the collection, maintenance, use, disclosure, or provision of access to the Covered Information;*

Provision V.E.3(e) *State whether and how Respondent will obtain consent from Users for the collection, maintenance, use, disclosure, or provision of access to Covered Information;*

Provision V.E.3(f) *Identify any privacy controls that will be provided to Users relevant to the collection, maintenance, use, disclosure, or provision of access to the Covered Information;*

Provision V.E.3(g) *Identify any third parties to whom Respondent will disclose or provide access to the Covered Information;*

Provision V.E.3(h) *Assess and describe the material risks to the privacy, security, confidentiality, and integrity of Covered Information presented by the product, service, or practice;*

Provision V.E.3(i) *Assess and describe the safeguards to control for the identified risks, and whether any additional safeguards need to be implemented to control for such risks;*

Provision V.E.3(j) *Explain the reasons why Respondent deems the notice and consent mechanisms described in Provisions V.E.3(d) and V.E.3(e) sufficient;*

Provision V.E.3(k) *Identify and describe any limitations on the collection, maintenance, use, disclosure, or provision of access to Covered Information based on: (i) the context of the collection of such Covered Information; (ii) notice to Users; and (iii) any consent given by Users at the time of collection or through subsequent authorization;*

Provision V.E.3(l) *Identify and describe any changes in how privacy and security-related options will be presented to Users, and describe the means and results of any testing Respondent performed in considering such changes, including but not limited to A/B testing, engagement optimization, or other testing to evaluate a User's movement through a privacy or security-related pathway;*

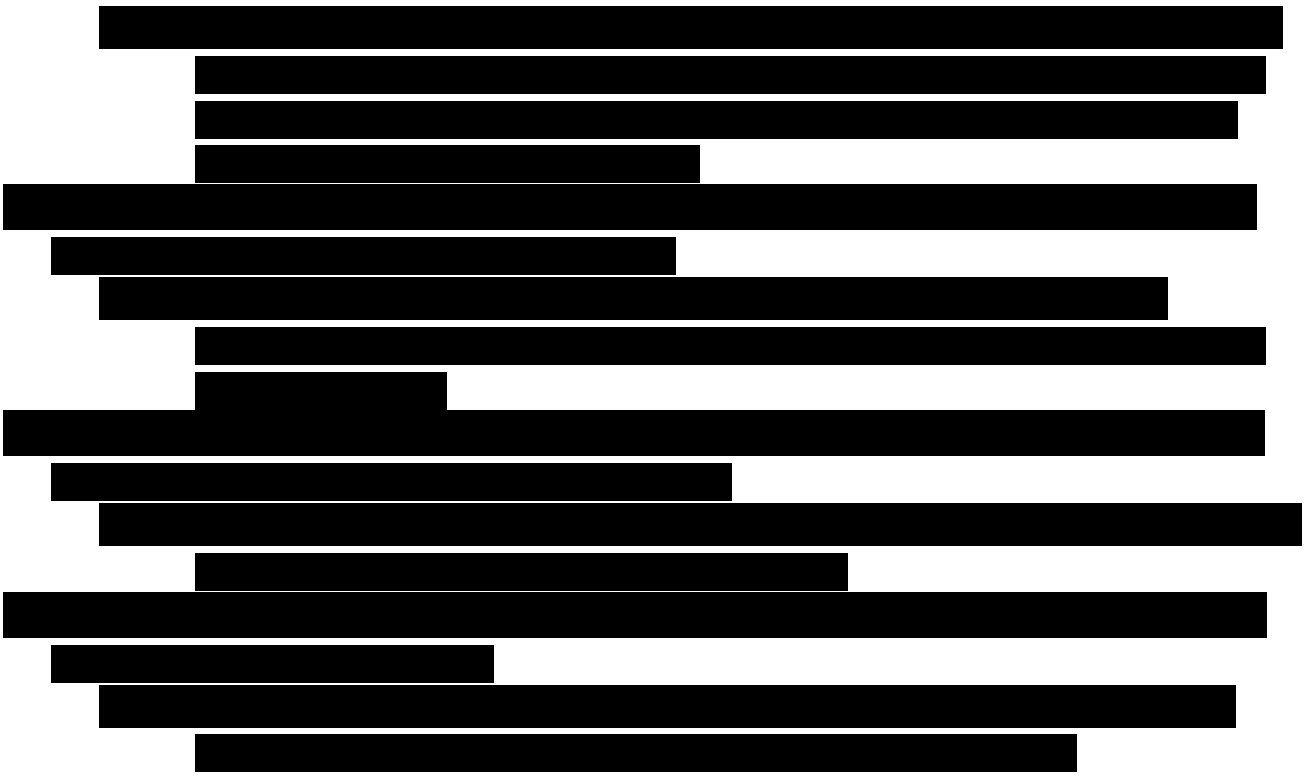
Provision V.E.3(m) *Include any other safeguards or other procedures that would mitigate the identified risks to the privacy, security, confidentiality, and integrity of Covered Information that were not implemented, and each reason that such alternatives were not implemented; and*

Provision V.E.3(n) *Include any decision or recommendation made as a result of the review (e.g., whether the practice was approved, approved contingent upon safeguards or other recommendations being implemented, or rejected);*

[redacted]

[redacted]

[2] Explain the reasons why Respondent deems the notice and consent mechanisms [described in Provisions V.E.3(d) and V.E.3(e)] sufficient;
[3] Include any other safeguards or other procedures that would mitigate the identified risks to the privacy, security, confidentiality, and integrity of Covered Information that were not implemented, and each reason that such alternatives were not implemented;



Provision V.E.4 *Safeguards to prevent the collection, maintenance, use, disclosure, or access to Covered Information beyond the limitations identified in Provision V.E.3(k), including:*

The Controls that make up Twitter's Information Security Program are designed to provide a defense-in-depth approach to preventing the collection, maintenance, use, disclosure, or access to Covered Information, including beyond the limitations identified in Provision V.E.3(k) for any particular product or service.

FTI's summary of findings pertaining to Provisions V.E.4(a)-(d) can be found below the following list of the Provisions.

Provision V.E.4(a) *Regular training, at least once a year, for any employees and independent contractors whose responsibilities include the collection, maintenance, disclosure, use, or provision of access to Covered Information, on the permissible collection, maintenance, disclosure, use, or provision of access to Covered Information and any related limitations;*

Provision V.E.4(b) *Written attestations by those employees and independent contractors that they will not collect, maintain, disclose, use, or provide access to the Covered Information in a manner inconsistent with those limitations;*

Provision V.E.4(c) *Designation of a senior officer, or senior level team composed of no more than five (5) persons, to be responsible for any decision to collect, maintain, use, disclose, or provide access to the Covered Information; and*

Provision V.E.4(d) *Treating any new method of collecting, maintaining, using, disclosing, providing access to, or deleting the Covered Information as a new or modified product, service, or practice requiring the reviews set forth in Provisions V.E.1-3;*

[redacted]

Provision V.E.5 *Regular privacy and information security training programs for all employees and independent contractors on at least an annual basis, updated to address any identified material internal or external risks and safeguards implemented pursuant to this Order;*

[redacted]

Provision V.E.6 *Technical measures to monitor Respondent's Resources to identify unauthorized attempts to: (a) access, modify, or exfiltrate Covered Information from Respondent's Resources; or (b) access or take over Users' accounts; and*

[redacted]

[redacted]

Provision V.E.7 *Data access policies and controls for all: (a) databases storing Covered Information; (b) Resources that provide access to Users' accounts; and (c) Resources containing information that enables or facilitates access to Respondent's internal network and systems;*

[redacted]

Provision V.F *Assess, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following the resolution of a Covered Incident, the sufficiency of any safeguards in place to address the internal and external risks to the privacy, security, confidentiality, or integrity of Covered Information, and modify the Program based on the results;*

[redacted]

[redacted]

Provision V.G *Test and monitor the effectiveness of the safeguards at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following the resolution of a Covered Incident, and modify the Program based on the results. Such testing and monitoring must include: (1) vulnerability testing of Respondent's network(s) once every four (4) months and promptly (not to exceed thirty (30) days) after an unauthorized intrusion into Respondent's Resources; and (2) penetration testing of Respondent's network(s) at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after an unauthorized intrusion into Respondent's Resources;*

[redacted]

Provision V.H *Select and retain service providers capable of safeguarding Covered Information they access through or receive from Respondent, and contractually require service providers to implement and maintain safeguards sufficient to address the internal and external risks to the privacy, security, confidentiality, or integrity of Covered Information; and*

[redacted]

Provision V.I *Evaluate and adjust the Program in light of any changes to Respondent's operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in Provision V.D of this Order, or any other circumstances that Respondent knows or has reason to believe may have an impact on the effectiveness of the Program or any of its individual safeguards. At a minimum, Respondent must evaluate the Program at least once every twelve (12) months and modify the Program based on the results.*

[redacted]

The table depicted in Section VI of this report represents the detailed analysis of FTI's Assessment. The table is composed of the following columns:

- **Control**, which identifies the Control number;
- **Control Activity**, which describes the intent of the Control;
- **Evidence and Testing**, which describes the evidence FTI considered and testing that occurred;
- **Result**, which outlines FTI's operating effectiveness opinion and potential consumer risk;
- **Recommendations**, as applicable, on a Control-by-Control basis; and
- **Order,** which identifies the specific requirement of the Order, if applicable, the Control is intended to satisfy.

FTI noted that not all Controls are aligned with a specific requirement of the Order because the Controls defined in the Program extend beyond the scope of the Order. The "Order" column of the table contained in Section VI reads "Not Mapped" for those Controls.

C. Summary Findings Related to Provision VI.D.3 of the Order

In this section, FTI identifies key gaps or weaknesses in the Program, as required by Provision VI.D.3 of the Order and, where relevant, makes recommendations to remediate or cure any such gaps and weaknesses.

[redacted]

[redacted] FTI notes that Twitter leadership has emphasized its promotion of a security and privacy-minded culture throughout the organization.

Gaps and Weaknesses and Recommendations

As part of our Assessment, we found targeted areas of improvement that, if implemented, would positively support the maturity or maintenance of the Program.

Privacy Risk Assessment: [redacted]

Internal Audit, Assessment and Testing, Program Resources: [redacted]

[redacted]

Data Retention and Deletion: [redacted]

Security and Privacy as Part of the Software Development Lifecycle: [redacted]

[redacted]

Employee Onboarding Procedures: [redacted]

[redacted]

Asset Management: [redacted]

[redacted]

[4] FTI notes that, as of the publication of this Assessment Report, [redacted]

D. Summary Findings Related to Provision VI.D.4 of the Order

This is the initial Assessment Report in accordance with Provision VI of the Order. As such, we did not address the status of gaps or weaknesses in, or instances of material non-compliance with, the Program that were identified in any prior Assessment required by the Order.

E. Summary Findings Related to Provision VI.D.5 of the Order

All evidence examined to make our determinations, assessments, and identifications can be found in Section VI, Control Activities, Evidence and Testing, Results, and Recommendations, of this Assessment. FTI did not rely solely on the assertions or attestations of Twitter's management. FTI interviewed relevant leadership and Control Owners and tested all information security and privacy Controls through the review of evidence. For certain Controls, we made note that evidence was only made available via screenshare sessions with Control Owners. While we encountered issues related to the lack of Control design documentation and, in some instances, lack of awareness on the part of Control Owners, based on the content and comprehensiveness of the information considered, we concluded that the evidence examined is sufficient to justify our findings.

IV. Assessment Approach

A. Methodology

To provide a complete Assessment, we developed a strategy that provided a standardized approach for planning and resourcing. We:

- Assigned dedicated resources suitable for completing the Assessment;
- Defined clear objectives and constraints;
- Scheduled defined events and deliverables;
- Developed testing procedures based on review of documentation and inquiry with Control Owners and Program leads;
- Analyzed risks based on threats and regulatory requirements we felt could impact an organization of Twitter's size, business scope, and complexity;
- Identified gaps and weaknesses, in order to recommend remediation actions; and
- Evaluated and assessed the Program through the lens of privacy and information security industry best practices and for compliance with the Order.

Assessment of each Control occurred throughout the reporting period and was dependent on the nature of the Control and its intended outcome. Therefore, as applicable, FTI used the following methodology to determine whether the Controls met or exceeded the protections required by Provision V of the Order:

Inquiry of Personnel and Examination of Evidence: Upon undergoing walkthroughs of each Control, we designed testing procedures and requested relevant evidence in accordance with those procedures. Upon receipt of evidence, we validated the design and operating effectiveness of each Control. Our inspection relied on: inquiry with Control Owners; screenshare sessions with Control Owners; documents, including but not limited to policies and procedures, risk assessments, training and awareness programs; and artifacts and demonstrable evidence, including but not limited to logs, screen captures, and network designs. We note that, because Twitter did not previously document operating effectiveness testing procedures or validate what evidence Twitter would expect to provide for each Control, we frequently had to submit additional clarifications and additional evidence requests. Evidence varied based on the Control, which was anticipated and appropriate. We collected and evaluated evidence from throughout the reporting period but primarily starting at November 7, 2022, from which point the Program was required to have been implemented. Upon thorough examination of the evidence, to validate the information presented, we interviewed personnel. A list of persons interviewed is presented as Appendix A.

When necessary, to validate evidence and to better understand the design of the Controls implemented, we submitted requests for information and performed additional testing.

Through our approach, we were able to:

1. Assess whether the Controls met or exceeded the protections required by the Order;
2. Assess whether the persons operating the Controls possessed the requisite knowledge, authority, and competence to operate the Controls effectively; and
3. Make an assessment regarding the overall operational design and effectiveness of the Program.

B. Independence

FTI acted as an independent third-party professional in conducting the Assessment. In the five years prior to the date of this Assessment, Twitter has not hired FTI for any other engagements pertaining to privacy or information security. FTI does not have any shared employees, directors, or officers with Twitter. The fees charged by FTI for this engagement are not contingent on the outcome of this matter or the opinions expressed throughout this report.

FTI and its engagement personnel sought to avoid any conflicts of interest, actual or perceived, that could impair our ability to provide the FTC and Twitter with an independent professional judgment. As part of the Assessment, FTI experts consulted with Twitter and its employees as necessary and exercised best professional judgment to maintain independence and ensure that our findings and conclusions remain as such.

To ensure ongoing independent oversight, review, and input into the methodology and execution of the Assessment, FTI has had privacy and information security professionals who were not involved with

the day-to-day activities of the Assessment and who have not directly interacted with any Twitter Personnel review the Assessment Report.

C. Qualifications

FTI Cybersecurity is an intelligence-led, expert-driven practice focused on providing strategic and operational solutions to global cybersecurity and privacy challenges. Our mission is to help organizations understand their information security and privacy environments, harden their defenses, improve their practices, meet regulatory requirements, rapidly and precisely hunt threats, holistically respond to crises, and sustainably recover their operations and reputation after an incident. Our seasoned experts bring deep technical and practical experience to the delivery of these solutions. Our industry experience in regulatory assessments, forensic investigations, incident response, strategic communications, crisis management, network defense operations, and expert testimony empowers FTI to meet a full range of technical needs across the globe.

Collectively, our cybersecurity and privacy professionals have backgrounds in law enforcement, intelligence, technology, national and international security, finance, policy and public affairs, fraud detection, incident response, crisis management and disaster recovery, strategic communications, forensics and litigation, and academia and training.

Certifications held by our professionals include Certified Information Systems Security Professional (“CISSP”); Certified Information Security Manager (“CISM”); Certified Information Systems Auditor (“CISA”); Certified Information Privacy Professional (“CIPP”); Certified Ethical Hacker (“CEH”); Global Information Assurance Certification Certified Incident Handler (“GCIH”); Global Information Assurance Certification Certified Enterprise Defender (“GCED”); and Global Information Assurance Certification Security Essentials (“GSEC”).

This Assessment was performed under the leadership of Ms. Tracy Wilkison, Senior Managing Director.

V. Twitter’s Information Security and Privacy Program Overview

Company Overview

On X, people are free to be their true selves, so long as they operate within the bounds of the law. Free expression and platform safety are not at odds. Our mission is to serve the public interest by facilitating an open exchange of accurate information and dialogue. And for that, we need to protect people's privacy. On X, people can consume, create, distribute and discover content about the topics and events they care about most.

X will become the global town square where the public gathers to pursue its passions. As we build this global town square with unlimited ways to interact, we’ll also create a marketplace that enables the economic success of all its participants.

X knows that we have a big responsibility to protect free expression. And we will continue to collaborate with all partners who want to preserve people's right to freely express themselves and equally to work to create a safe and healthy space for everyone.

Governance Description

X is committed to ensuring that the Personal Data entrusted to us is used only in the pursuit of X's mission to protect public conversations and foster customer trust in X. X aims to do that in ways that preserve the integrity, privacy, security, and confidentiality of the data, while securing rights and freedoms of individuals. X's vision is to bring a customer-first lens to X's data and privacy decisions so that we meet our promises to customers and regulators.

[redacted]

Selection of the Framework

[redacted]

[redacted]

PROGRAM SCOPE

[redacted]

RISK ASSESSMENT

[redacted]

[redacted]

MONITORING AND VERIFICATION

[redacted]

VI. Control Activities, Evidence and Testing, Results, and Recommendations

[Omitted]

Appendix A: Interviewees

In addition to holding walkthroughs and working sessions with all Control Owners and relevant Program team members, FTI interviewed the following Twitter Personnel with responsibilities to the Program:

Linda Yaccarino, Chief Executive Officer;

Renato Monteiro, Global Data Protection Officer;

Christopher Stanley, Head of Security Engineering;

Anoop Sukumaran, Access Engineering;

Damian Vogt, Privacy Program Manager;

Jibran Hussain, PDP Operations Lead;

Luiz Mendes de Mello, Detection and Response Team;

Mary Hansbury, Employment Legal Lead;

Naser Baseer, Product Counsel;

Walter Dodge, Security Governance, Risk, and Compliance; and

Xiapei Wang, Privacy Engineering.

Appendix B: Relevant Screen Captures

[Omitted]